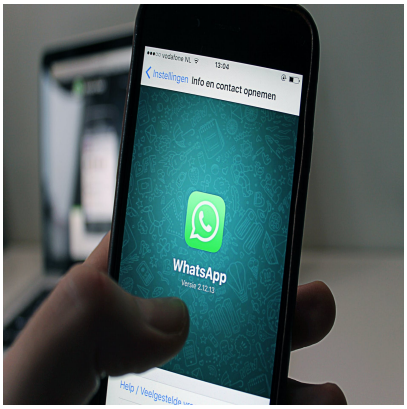

WhatsApp: Une firme israÃ©lienne est Â« largement impliquÃ©e Â» dans le hacking de nos utilisateurs

Description

The Guardian : Le groupe NSO serait liÃ© au piratage de 1 400 personnes dont des militants des droits humains

Photo par **Anton** @ **Pexels**

Par The Guardian, 29 avril 2020

WhatsApp a avancÃ©, dans une nouvelle action en justice, quâ??une sociÃ©tÃ© israÃ©lienne dâ??espionnage informatique avait utilisÃ© des serveurs basÃ©s aux Ã?tats Unis et Ã©tait Â« *largement impliquÃ©e* Â» dans des piratages de tÃ©lÃ©phones mobiles appartenant Ã 1 400 utilisateurs de WhatsApp, dont des hauts fonctionnaires du gouvernement, des journalistes et des militants des droits humains.

Les nouveaux arguments sur le groupe NSO mettent en avant que cette sociÃ©tÃ© israÃ©lienne porte la responsabilitÃ© de graves violations de droits humains, dont le piratage de plus dâ??une douzaine

de journalistes indiens et de dissidents rwandais.

Depuis des annÃ©es le groupe NSO dit que son logiciel espion est achetÃ© par des gouvernements dans le but de pister des terroristes et autres criminels et quâ??il nâ??a pas de connaissance propre de la faÃ§on dont ces clients â?? dont il est dit que lâ??Arabie Saoudite et le Mexique ont fait partie dans le passÃ©â?? utilisent son logiciel dâ??espionnage et de piratage.

Mais une action en justice intentÃ©e lâ??an dernier par WhatsApp contre le groupe NSO â?? la premiÃ¨re de la sorte de la part dâ??une importante entreprise de technologie â?? rÃ©vÃ¨le dâ??autres dÃ©tails techniques sur la faÃ§on dont PÃ©gase, le logiciel espion, est supposÃ©ment dÃ©ployÃ© contre des cibles.

Dans les documents prÃ©sentÃ©s au tribunal la semaine derniÃ¨re, WhatsApp a dit que sa propre enquÃªte sur la faÃ§on dont PÃ©gase avait Ã©tÃ© utilisÃ© contre 1 400 clients lâ??annÃ©e derniÃ¨re, montrait que des serveurs contrÃ´lÃ©s par le groupe NSO, et non par ses clients gouvernementaux, faisaient intÃ©gralement partie de la faÃ§on dont les piratages Ã©taient rÃ©alisÃ©s.

WhatsApp a dit que les victimes de piratage avaient reÃ§u des appels tÃ©lÃ©phoniques utilisant son application de messagerie et Ã©taient infectÃ©s par PÃ©gase. Puis, a-t-il dit, Â« *NSO a utilisÃ© un rÃ©seau dâ??ordinateurs pour contrÃ´ler et mettre Ã jour PÃ©gase une fois quâ??il a Ã©tÃ© implantÃ© dans les appareils des utilisateurs. Ces ordinateurs contrÃ´lÃ©s par NSO ont servi de centre nodal Ã partir duquel NSO contrÃ´lait le fonctionnement et lâ??utilisation de PÃ©gase par ses clients* Â».

Selon le document de WhatsApp, NSO a obtenu Â« un accÃ¨s non autorisÃ© Â» Ã ses serveurs par une ingÃ©nierie inverse de lâ??application de messagerie, puis en Ã©vitant les fonctions de sÃ©curitÃ© de WhatsApp qui empÃªchent la manipulation des caractÃ©ristiques des appels de cette sociÃ©tÃ©. Un ingÃ©nieur de WhatsApp qui a enquÃªtÃ© sur les piratages a dit dans une dÃ©claration sous serment devant le tribunal que, dans 720 cas, lâ??adresse IP dâ??un serveur distant Ã©tait incluse dans le code malveillant utilisÃ© dans les attaques. Le serveur distant, a dit lâ??ingÃ©nieur, Ã©tait basÃ© Ã Los Angeles et appartenait Ã une sociÃ©tÃ© dont le centre de donnÃ©es Ã©tait utilisÃ© par NSO.

NSO a dit dans des documents lÃ©gaux quâ??il nâ??a pas moyen de connaitre la faÃ§on dont les clients utilisent ses outils de piratage et donc quâ??il ne sait pas qui est ciblÃ© par des gouvernements.

Mais, un expert de Citizen Lab, John Scott-Railton, qui a travaillÃ© avec WhatsApp sur ce problÃ¨me, a dit que le contrÃ´le par NSO des serveurs impliquÃ©s dans le piratage, suggÃ¨re que lâ??entreprise aurait eu des registres, dont des adresses IP, permettant dâ??identifier les utilisateurs qui Ã©taient ciblÃ©s.

Â« *Que NSO consulte ou non ces registres, qui sait ? Mais le fait que cela ait pu Ãªtre fait contredit leurs dÃ©clarations* Â» a dit Scott-Railton.

Dans une dÃ©claration faite au *Guardian*, NSO sâ??en est tenu Ã ses prÃ©cÃ©dentes remarques. Â« *Nos produits sont utilisÃ©s pour faire barrage au terrorisme, pour faire baisser la criminalitÃ© violente, et pour sauver des vies. Le groupe NSO ne fait pas fonctionner le logiciel PÃ©gase pour ses*

clients Â» a dit lâ??entreprise. Â« Nos dÃ©clarations prÃ©cÃ©dentes concernant notre activitÃ© et lâ??ampleur de notre interaction avec les services de renseignement de notre gouvernement et avec les agences clientes chargÃ©es du respect de la loi, sont exactes Â».

Lâ??entreprise a dit quâ??elle ferait parvenir sa rÃ©ponse au tribunal dans les prochains jours.

Les nouveaux Ã©lÃ©ments sur ce cas interviennent alors que NSO est confrontÃ© Ã dâ??autres questions sur la pertinence dâ??un produit de traÃ§age quâ??elle a lancÃ© suite Ã lâ??irruption de COVID-19. Le nouveau programme, appelÃ© Fleming, utilise des donnÃ©es de tÃ©lÃ©phones portables et de lâ??information sur la santÃ© publique pour identifier avec qui des individus infectÃ©s par le coronavirus peuvent avoir Ã©tÃ© en contact. Un rapport de NBC de la semaine derniÃ¨re disait que la marque de fabrique du nouvel outil de NSO Ã©tait amÃ©ricaine.

Mais dans un tweet, Scott-Railton a dit que son analyse montrait que ce systÃ¨me reposait sur des donnÃ©es paraissant trÃ¨s imprÃ©cises.

Â« *Quand on travaille avec des donnÃ©es incorporant beaucoup dâ??inexactitude, il serait un peu fort de lancer des alertes chaque fois que cela sâ??est produit. Ou dâ??exiger des mises en quarantaine. Les taux de faux rÃ©sultats positifs obtenus crÃ¨veraient le plafond. Maisâ?¦ il en serait de mÃªme pour les faux rÃ©sultats nÃ©gatifs* Â» a-t-il dit.

https://twitter.com/jsrailton/status/1254198212430368769

QuestionnÃ© sur ces tweets, NSO a dit que ces Â« *demandes infondÃ©es* Â» Ã©taient basÃ©es sur Â« *des suppositions et des captures dâ??Ã©crans obsolÃ¨tes plutÃ´t que sur des faits* Â».

Â« *Pendant ce temps, Fleming, notre produit COVID-19, sâ??est avÃ©rÃ© vital pour des gouvernements dans le monde entier, qui travaillent Ã contenir lâ??Ã©pidÃ©mie. Des journalistes trÃ¨s respectÃ©s dans plusieurs pays ont vu Fleming, ont compris comment fonctionne la technologie et ont reconnu quâ??elle relÃ¨ve de la toute derniÃ¨re Ã©volution dans les logiciels dâ??analyse, qui ne compromettent pas la vie privÃ©e* Â» a dit lâ??entreprise.

Traduction : SF pour lâ??Agence MÃ©dia Palestine

Source : The Guardian

date crÃ©Ã©e
2020/04/30